Amendment to the Specification

In the specification, replace paragraph 57 with the following paragraph:

As shown in FIG. 4, a user 1 shopping at an online merchant's website, adds items to the online shopping cart. The user chooses to checkout and is provided with the merchant's payment page (STEP 501). The form of the payment page is sent from the merchant's website 210 to the user's browser 11 and includes JavaScript and VBScript to detect the presence of a smart card reader 12. If the reader software is detected, then the user 1 is shown the "Use SCP" option, which invokes the smart card payment (SCP) process (STEP 502). The user 1 selects the "Use SCP" option, which causes the user browser 11 to be directed to the host system 300 user interface 310 (*e.g.*, web server) (STEP 503a) and then to the smart card payment (SCP) system 330 (STEP 503b). The SCP system 330 may include, as appropriate, application servers and databases for processing, storing and managing data. The SCP system 330 saves the user 1 request and redirects the user's browser to an authentication system 320 for appropriate sign-on and authentication (STEPS 504a-d). The authentication system 320, via a suitable sign-on routine, obtains a challenge string from an appropriate user database system 340 (STEP 505). The user 1 is challenged to insert his or her smart card 14 into the smart card reader 12 and enter the appropriate PIN (STEPS 506a-b) – although, as previously noted, any suitable authentication technique is appropriate. In this exemplary embodiment, the user 1 enters the PIN, resulting in the challenge string being signed and returned, with a digital certificate, to the host system authentication system 320 (STEP 507a-b). The digital certificate and the signed challenge string is passed to the user database system 340 where the user 1 is identified from within various user and/or account information database tables (STEP 508). The user may thus be authenticated by comparing the digital certificate to the signed challenged string or by comparing either the digital certificate or the signed challenged string to a third data set stored in the user and/or account information database tables. It should be appreciated that the data structure may be configured in any number of suitable ways, comprising a plurality of servers and databases as desired. The authentication system 320 signs the user a into the host system's security system 350 that facilitates the secure exchange of data between servers and databases (STEP 509).